

1 --20. A method for protecting the processing of sensitive information in a
2 security module having a monolithic structure, information processing means
3 (31) and storage means for storing (32,33) information capable of being
4 processed by said processing means, comprising the following steps:

- 5 - selecting a piece of sensitive information stored in the storage means;
6 - determining a specific condition for the integrity of said information;
7 - reading the information and transmitting it to the processing means for
8 processing;
9 - processing the information and verifying during processing that the
10 specific condition is satisfied; and
11 - disabling processing of the information if the specific condition is not
12 satisfied.

1 21. The method according to claim 20, wherein the information is an
2 operation code read in the storage means (32, 33), the operation code being
3 contained in a table having a content determined during the manufacture of the
4 security module, and the specific condition for the integrity of the information
5 being the value of the information is equal to one of several set values.

1 22. The method according to claim 21, wherein the operation code to
2 be processed is coded in the form of data bits and said bits do not all have the
3 same binary value.

1 23. The method according to claim 20, wherein the specific step of
2 determining the condition for the integrity of said information comprises checking
3 a calculated or first piece of integrity data using the information read in the
4 storage means (32, 33) during the reading of the information and transmitting the
5 first piece of integrity data to the processing means, and calculating a second
6 piece of integrity data by the processing means from the information received
7 and checking for equality between the first and second pieces of integrity data.

1 24. The method according to claim 23, wherein the first piece of
2 integrity data is calculated from at least one piece of calculation data whose
3 value varies as a function of time.

1 25. The method according to claim 23, wherein the first piece of
2 integrity data is calculated from at least one piece of calculation data whose
3 value varies randomly.

1 26. The method according to claim 20, wherein the disabling of the
2 processing of the information is performed by a microprogrammed instruction.

1 27. The method according to claim 26, wherein the microprogrammed
2 instruction performs the following steps:

- 3 - writing a piece of disable data into a nonvolatile location of the storage
4 means (32, 33); and
5 - disabling the processing of the information.

1 28. The method according to claim 27 further comprising reading by
2 the processing means (31) a nonvolatile location of the storage means (32, 33)
3 upon power up of said module and disabling the module if a value read at this
4 location does not match.

1 29. A security module comprising an electronic circuit having a
2 monolithic structure and comprising information processing means (31) and
3 information storage means (32, 33), means for extracting information from the
4 storage means and means for selecting information to be processed, the
5 processing means further comprising means for verifying a specific integrity
6 condition of a piece of sensitive information, and means for disabling the
7 processing of the information, said means for disabling being activated when the
8 means for verification have detected that the specific condition is not satisfied.

2 the parity generators (7, 8) varies randomly.

37 A security module according to claim 33, characterized in that the

2 irreversible writing of the indicator into the storage means (32, 33) is performed
3 by executing a microprogrammed instruction.

1 38. A security module according to claim 29, characterized in that the
2 security module is a microcircuit card.--

Year	1970	1971	1972	1973	1974	1975	1976	1977	1978	1979	1980	1981	1982	1983	1984	1985	1986	1987	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	2037	2038	2039	2040	2041	2042	2043	2044	2045	2046	2047	2048	2049	2050	2051	2052	2053	2054	2055	2056	2057	2058	2059	2060	2061	2062	2063	2064	2065	2066	2067	2068	2069	2070	2071	2072	2073	2074	2075	2076	2077	2078	2079	2080	2081	2082	2083	2084	2085	2086	2087	2088	2089	2090	2091	2092	2093	2094	2095	2096	2097	2098	2099	2100
1970	1971	1972	1973	1974	1975	1976	1977	1978	1979	1980	1981	1982	1983	1984	1985	1986	1987	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	2037	2038	2039	2040	2041	2042	2043	2044	2045	2046	2047	2048	2049	2050	2051	2052	2053	2054	2055	2056	2057	2058	2059	2060	2061	2062	2063	2064	2065	2066	2067	2068	2069	2070	2071	2072	2073	2074	2075	2076	2077	2078	2079	2080	2081	2082	2083	2084	2085	2086	2087	2088	2089	2090	2091	2092	2093	2094	2095	2096	2097	2098	2099	2100	